Brontok.22, Varian Terbaru yang Kembali Dirilis

csrss.exe
lsass.exe
services.exe

File Folder
File Folder
Application

Brontok yang menyamar sebagai folder.

Siapa yang tak kenal Brontok? Mungkin Anda semua sebagai pengguna komputer sudah sering mendengar informasi mengenai virus Brontok ini, atau bahkan komputer Anda sudah terinfeksi Brontok?

Arief Prabowo

Setelah meraih sukses dari Brontok terdahulu, kini JowoBot Community, yang ditengarai sebagai pembuat virus ini telah mengeluarkan rilis terbaru dari Brontok, yakni Brontok.22 atau dikenal juga dengan nama Mybro.

Apa *aja sih* perbedaannya dengan Brontok versi terdahulu? Jika dilihat secara fisik, memang tidak terlalu kelihatan adanya perbedaan, yakni masih menggunakan icon folder. Tapi apabila dilihat secara mendalam, yakni dengan "membongkar" sang virus, akan terlihat perbedaan yang cukup besar. Yakni dari segi pemrogramannya, yang dahulu menggunakan bahasa Visual Basic, kini kami duga beralih ke C++. Ini bisa dilihat dari badan virus yang menggunakan run time library milik C++. Diyakini pembuat virus ini memang selalu memperkuat virus buatannya agar dapat selalu bertahan hidup.

Social Engineering

Seperti halnya yang dilakukan oleh pendahulunya, Brontok.22 atau MyBro ini sepertinya sudah menyebar luas di masyarakat. Ia memiliki kemampuan *social engineering* atau rekayasa sosial yang sangat bagus. Social engineering yang dimaksud di sini adalah kemampuannya untuk mengamuflasekan diri sebagai sebuah folder, yaitu dengan memanfaatkan icon folder sebagai icon program virus.

Informasi Brontok pada registry.

Brontok akan membaca teks pada *Title Bar* program yang aktif, apabila program itu mengganggu, maka akan disingkirkannya.

Bagaimana Brontok Menyebar?

Brontok dapat menyebar melalui media disket, flash disk, dan e-mail, yang notabene merupakan media yang paling banyak digunakan oleh pengguna komputer di Indonesia. Selain itu apabila komputer terhubung dengan jaringan, dia akan meng-*copy*-kan dirinya ke setiap folder yang di-*share*.

Brontok mengumpulkan setiap alamat e-mail yang ditemukannya dari file-file dengan ektensi .ppt, .cfm, .eml, .txt, .xls, .doc, .pdf pada direktori yang telah ditentukannya. Setelah terkumpul, maka ia akan segera mengirimkannya menggunakan SMTP *engine* miliknya sendiri agar dapat mengirimkannya secara massal. *Attachment* yang dikirim berupa sebuah trojan downloader, yang apabila penerima e-mail tersebut mengeksekusinya, maka program tersebut akan memonitor akses Internet dan akan berusaha men-*download* file dari situs tertentu, yang sebenarnya file tersebut adalah virus yang asli.

Bermain dengan Registry

Registry merupakan tempat favorit para virus, karena merupakan salah satu komponen

```
Command Bro !!!
########################## BRONTOK.C[22] ##########################

-- Hentikanlah kebobrokan di negeri ini --

1. Penjarakan Koruptor, Penyelundup, Tukang Suap, & Bandar NARKOBA
                < Send To NUSAKAMBANGAN >

2. Stop Free Sex, Aborsi, & Prostitusi
                < Go To HELL >

3. Stop Pencemaran Alam, Pembakaran Hutan & Perburuan Liar.

4. SAY NO TO DRUGS !!!

-- Spizaetus Cirrhatus --

[   By JowoBot   ]
```

Pesan yang disampaikan oleh si empunya Brontok.

```
Command Bro !!!
~~ Sedikit Jawaban  u/ Membungkam Mulut Sesumbar 'Mereka' ~~

Nobron & Romdil = Otak Kosong, Mulut Besar, Cuma Bisa Baca Puisi

Nobron = Satria Dungu = Nothing !!!

Romdil = Tukang Jiplak = Nothing !!!

Nobron & Romdil -->> Kicked by The Amazing Brontok

[   By JowoBot   ]_
```

Pesan yang ditujukan kepada virus lain.

penting dalam Windows. Perubahan yang dilakukan oleh virus ini salah satunya, yaitu dengan men-*disable* Registry Editor. Pada Brontok.22 kali ini Folder Options tidak di-*disable* seperti pada Brontok terdahulu, hanya saja kita tetap tidak bisa mengaksesnya, karena virus ini akan segera men-*terminate* process explorer.exe yang merupakan Shell dari Windows. Hal ini juga terjadi apabila kita mengakses Schedule Tasks. Dengan mengubah registry, virus ini juga mengeset agar tidak menampilkan ekstensi dari setiap file dan menyembunyikan file-file *hidden* dan system.

Tapi, perubahan yang paling berpengaruh di sini adalah adanya penambahan *value* pada beberapa *section* di registry yang dijadikan sebagai *autorun*. Salah satunya pada HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Dan tak lupa ia juga menginfeksi value untuk run in safe-mode, yaitu pada HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell, dengan mengalihkan nilai dari value tersebut ke program utama virus. Ini artinya virus ini dapat aktif walaupun dalam modus safe-mode.

Aktif di Memory

Setiap kali *start* Windows virus akan aktif di memory. Process name yang digunakan menyerupai nama-nama service di Windows, contohnya csrss.exe, lsass.exe, dan smss.exe, juga beberapa process dengan nama random. Apabila kita ingin meng-*kill* process tersebut dari Task Manager, sepertinya tidak bisa dilakukan, karena Brontok juga akan memblok akses ke Task Manager.

Apa sih yang Ia Perbuat?

Selain pada registry, perubahan lain juga dilakukan pada file hosts milik Windows. File hosts ini dipergunakan oleh Windows untuk me-*resolve* atau menerjemahkan *hostname* menjadi alamat IP. Yang dilakukan Brontok adalah dengan cara mengalihkan setiap IP dari *hostname* atau alamat situs Internet ke IP 127.0.0.22. Angka 22 pada IP tersebut menunjukan versi dari Brontok.

Schedule Task juga tak luput dari serangan Brontok, ia akan menambahkan dua item baru dengan nama AT1 dan AT2 yang akan menjalankan file \Documents and Settings\%username%\Local Settings\Application Data\jalak-%random%-bali.com setiap hari pada pukul 11:03 dan 17:08.

Tak hanya itu, ia juga akan me-*rename* file Run-Time Library milik Visual Basic, yaitu MSVBVM60.DLL menjadi MSVBVM60.DLL.XXX, dimana XXX adalah nomor acak. Tujuannya adalah untuk mematikan virus-virus lain dan virus-virus Brontok versi lama yang masih diprogram menggunakan Visual Basic. Namun, tindakan ini juga membuat aplikasi–aplikasi yang diprogram menggunakan Visual Basic tidak akan dapat berjalan.

Jangan panik bila program antivirus Anda tidak bekerja dalam menghadapi virus ini, karena memang dimulai dari Brontok terdahulu, ia akan selalu mencoba untuk menyingkirkan program-program antivirus atau *security* yang terdapat pada komputer korban. Dan data seputar program apa saja yang ia singkirkan tersebut akan selalu di-*update* pada varian-varian berikutnya.

Virus ini juga akan menambahkan semacam "tanda pengenal"-nya pada registry. Apabila komputer terinfeksi, maka ia akan menuliskan beberapa *value* pada registry HKEY_CURRENT_USER\Software\Brontok. Value tersebut, di antaranya Dedicated 2, Developer, Released, Message, dan Version.

Di samping niat jahatnya, virus ini juga memiliki "niat baik", yaitu dapat menghapus virus lain, contohnya RomanticDevil, NoBron, dan beberapa virus lokal lainnya. Tapi tidak mungkin *kan* kita menggunakan virus untuk dapat membasmi virus? Karena, walau bagaimanapun, yang namanya virus pasti merugikan. Iya *gak*? Selain itu, ada beberapa pesan yang menarik yang ditampilkan oleh virus ini. Brontok .22 ini akan membuat sebuah file teks pada root direktori dengan nama "Baca Bro !!!.txt", apabila kita mengklik file ini, maka Brontok akan membaca *caption* dari file yang dibuka dengan notepad tersebut, lalu menutup notepad-nya dan menampilkannya dalam modus Command Prompt. Salah satu pesan tersebut ditujukan untuk virus RomanticDevil dan NoBron. Apakah ini awal terjadinya perang virus?

Polymorphic?

Dari contoh virus yang kami punya, Brontok.22 ini memiliki nilai *hashing* yang berbeda-beda. Kami pikir ini varian yang berbeda-beda, atau memang virus ini memiliki kemampuan *polymorphic*?

Setelah ditelusuri, ternyata *name sections* pada *executable*-nya yang selalu berubah-ubah. Inilah yang mengakibatkan *hashing*-nya selalu berbeda. Tentu saja ini dilakukannya agar mempersulit antivirus dalam mendeteksi virus ini. Brontok juga di-*compress* menggunakan tool exe compressor, yang kemungkinan menggunakan UPX dan UPX Scrambler.

Cara Membasmi

Pembersihan secara manual Brontok.22 ini sepertinya cukup kompleks, karena virus ini telah menginfeksi berbagai sektor penting dari Windows, sehingga mempersulit kita untuk menghapus virus ini secara manual, terlebih lagi untuk orang awam.

Oleh karena itu, kami tim PC Media Antivirus telah meng-*update* program dan database dari PC Media Antivirus agar dapat mengenali dan membasmi virus ini secara tuntas dan akurat hingga 100%. ■